UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/695,008	10/28/2003	Steve W. Rodgers	15128US02	4253

23446 7590 09/21/2010

MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

EXAMINER	
HOANG, DANIEL L	
ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
09/21/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/695,008	RODGERS ET AL.	
	Examiner	Art Unit	
	DANIEL L. HOANG	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *2/26/10, 7/22/10*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22,38-51 and 54-57* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22, 38-51, 54-57* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 2/26/10 has been entered.

Election/Restrictions

Applicant's election without traverse of claims 1-22, 38-51, 54-57 in the reply filed on 7/22/10 is acknowledged.

Response to Arguments

Applicant's arguments filed 2/26/10 have been fully considered but they are not persuasive. Amended and newly added claims are treated below in the 103 rejection.

CLAIM REJECTIONS

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-22, 38-51, and 54-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rarick, US PGP No. 20050010527, and further in view of Perego et al., US Patent No. 6826663 and further in view of Watanabe et al., US Patent No. 7284133.

As per claim 1:

Rarick teaches:

A system for protecting data, comprising:

a memory in which encrypted data is stored; and

[see fig. 11A, Register Unit]

[see paragraph 84, "encryption circuit stores array values in a register unit"]

a processor coupled to the memory, the processor comprising a decryptor that decrypts the encrypted data,

[see paragraph 13, "In addition to being used for encrypting information, the method and apparatus may also be used for decrypting information."]

the decryptor being adapted to:

variably bit roll the encrypted data based on at least a data address,

[see paragraph 32, "swap" is viewed as analogous to the claimed "bit roll"]

to fixedly bit shuffle the bit-rolled data,

[see paragraph 33, "shift" is viewed as analogous to the claimed "bit shuffle"]

Rarick is mute in teaching that the decryptor is adapted to:

to add a first key to the bit-shuffled data and

For the above limitation, examiner relies upon the Perego reference. Perego teaches a method of adding a mask key to data by adding mask key bits into successive iterations of data (see col. 14, lines 4-36). It would have been obvious to one of ordinary skill in the art to utilize that which is taught by Perego to improve upon the invention cited above by Rarick in order to protect the integrity of the data while maintaining an acceptable tradeoff in latency.

The combination of the Rarick and Perego references is still mute in teaching that the decryptor is adapted to process the added data with a second key. For this limitation, examiner relies on the Watanabe reference. Watanabe teaches an information processing unit that encrypts data that is being stored in a memory device or that is newly generated, and stores the encrypted data in the memory device (see col. 5, paragraph 1). In particular relevance to the above limitation, Watanabe teaches changing the key data periodically or randomly and processing the data with the newly changed key. It would be obvious to one or ordinary skill in the art to modify the Rarick and Rarick inventions above in order to process data with a changed key so that the decrypted data can be protected against external attack, resulting in improved security (see col. 5, lines 15-18).

wherein the processor receives an original key and the data address,

[see above wherein the processor comprises a decryptor and wherein Perego teaches that the decryptor is adapted to add a first key to the bit shuffled data. The mask key taught by Perego above is viewed as the claimed "original key". See also above wherein Rarick teaches variably bit rolling the encrypted data based on an address. It is clear that the processor must receive an address because the processor comprises a decryptor that performs the bit rolling.]

wherein the processor generates multiplexer selection bits and the first key that is a shifted version of the original key based on the original key and data address,

[see Rarick, paragraph 11]

wherein the decryptor is adapted to variably bit roll the encrypted data by rotating bits within particular roll regions of encrypted data based on the multiplexer selection bits.

Paragraph 34 of the specification cites, "the bit roller may then perform a bit rolling operation. A bit rolling operation may include, for example, rotating bits within particular roll regions of the incoming data." Paragraph 32 of the Rarick reference teach the swap operation. Rarick teaches "the value present in the S[3] array position is written into the S[2] position, the value in the S[2] position is written into the S[1] position, the value in the S[1] position is written into the S[0] position, and so on." Examiner contends that this shifting of the values in the array is analogous to the "rotating bits" as cited in applicant's specification.

As per claim 2, Rarick teaches:

The system according to claim 1, wherein the decryptor is adapted to perform a single pipeline stage decryption.

[see paragraph 78]

As per claim 3, Rarick teaches:

The system according to claim 1, wherein the decryptor comprises a bit roller that rotates data in one or more roll regions of the incoming data based on an address related to the received encrypted data and a key related to the first key.

[see paragraph 35, table 3]

As per claim 4, Rarick teaches:

The system according to claim 3, wherein the key comprises a shifted version of the first key.

[*see paragraph 32]*

As per claim 5, Rarick teaches:

The system according to claim 3, wherein the bit roller comprises a plurality of multiplexers.

[see paragraph 11]

As per claim 6, Rarick teaches:

The system according to claim 5, wherein each multiplexer comprises a multiplexer selection input, wherein multiplexer selection bits are input at the multiplexer selection input, and wherein the multiplexer selection bits are generated based on the address related to the received encrypted data and the key related to the first key.

[see paragraph 11]

As per claim 7, Rarick teaches:

The system according to claim 1, wherein the decryptor comprises a fixed bit shuffler.

[see paragraph 43]

As per claim 8, Rarick teaches:

The system according to claim 7, wherein the fixed bit shuffler comprises a fixed, hard-coded bit shuffler.

[see paragraph 44]

As per claim 9, Rarick teaches:

The system according to claim 7, wherein the fixed bit shuffler does not add a gate delay to the decryptor.

[see paragraph 55]

As per claim 10, 44, Rarick teaches:

The system according to claim 1, wherein the decryptor comprises one or more two-bit adders.

[see paragraph 40]

As per claim 11, Rarick teaches:

The system according to claim 10, wherein each two-bit adder comprises three exclusive OR (XOR) gates and an AND gate.

[see paragraph 40]

As per claim 12, Rarick teaches:

The system according to claim 1, wherein the decryptor comprises an XOR block.

[see paragraph 40]

As per claim 13, Rarick teaches:

The system according to claim 12, wherein the XOR block comprises one or more XOR gates.

[see paragraph 69]

As per claim 14, Rarick teaches:

The system according to claim 13, wherein each XOR gate comprises a first input and a second input, the first input receiving a bit of the second key, the second input receiving a bit of the added data.

[see paragraph 69]

As per claim 15, Rarick teaches:

The system according to claim 1, wherein the first key is a shifted version of a key.

[see rejection of claim 3]

As per claim 16, Rarick teaches:

The system according to claim 15, wherein an amount of shift in the first key is based on an address related to the received encrypted data.

[see paragraph 36]

As per claim 17, Rarick teaches:

The system according to claim 15, wherein the first key is generated substantially in parallel with the decrypting of the encrypted data.

[see paragraph 30]

As per claim 18:

The system according to claim 1, wherein the decryptor does not add a latency to a processor pipeline.

[see rejection of claim 1]

As per claim 19:

The system according to claim 1, wherein the decryptor does not add enough gate delays to exceed a clock cycle budget of the processor.

[see rejection of claim 1]

As per claim 20, Rarick teaches:

The system according to claim 1, wherein the decryptor decrypts a word of the encrypted data in a single cycle.

[see paragraph 90, table 13]

As per claim 21, Rarick teaches:

The system according to claim 1, wherein the word comprises a 64-bit word.

[see paragraph 5]

As per claim 22, Rarick teaches:

The system according to claim 1, wherein the decryptor is adapted to receive encrypted data from the memory.

[see rejection of claim 1]

As per claim 23, Rarick teaches:

A system for protecting data, comprising: a memory in which encrypted data is stored; and a processor coupled to the memory, the processor comprising a decryptor that decrypts the encrypted data without adding a latency to a processor pipeline.

[see rejections of claim 1 and 18]

As per claim 24, Rarick teaches:

The system according to claim 23, wherein the decryptor decrypts the encrypted data without adding enough gate delays to exceed a clock cycle budget of the processor.

[see rejections of claim 1 and 19]

As per claim 25, Rarick teaches:

The system according to claim 23, wherein the decryptor decrypts the encrypted data and decrypts a word of the encrypted data in a single cycle.

[see rejections of claims 1 and 20]

As per claim 26, Rarick teaches:

A system for securing data, comprising: a processor that decrypts encrypted data, the processor being adapted to variably bit roll encrypted data and to fixedly bit shuffle the bit-rolled data.

[see rejection of claim 1]

As per claim 27, Rarick teaches:

The system according to claim 26, wherein the processor is adapted to perform a single pipeline stage decryption.

[see rejections of claim 26 and 2]

As per claim 28, Rarick teaches:

A system according to claim 26, wherein the processor is adapted to add a first key to the bit-shuffled data and to process the added data with a second key.

[see rejection of claim 1]

As per claim 29, Rarick teaches:

The system according to claim 26, wherein the processor is adapted to decrypt the encrypted data without adding a latency to a processor pipeline.

[see rejection of claim 18]

As per claim 30, Rarick teaches:

A method for securing processor instructions, comprising: variably rolling data information based on a first key and an address related to the data information; and hard-coded shuffling of the rolled data information; using one or more keys to process the data information.

[see rejections of claims 1, 3, and 8]

As per claim 31, Rarick teaches:

The method according to claim 30, wherein the rolling, the shuffling and the using are part of a single pipeline stage decryption.

[see rejection of claim 2]

As per claim 32, Rarick teaches:

The method according to claim 30, wherein using one or more keys to process the data information comprises adding the hard-coded data information and a shifted version of the first key.

[see rejections of claim 4 and 8]

As per claim 33, Rarick teaches:

The method according to claim 32, wherein using one or more keys to process the data information comprises processing the added data information with a second key using exclusive OR (XOR) gates.

[see rejection of claim 11]

As per claim 34, Rarick teaches:

The method according to claim 33, wherein the first key is unrelated to the second key.

[see rejection of claim 3]

As per claim 35, Rarick teaches:

The method according to claim 30, wherein the data information comprises encrypted data information.

[see rejection of claim 1]

As per claim 36, Rarick teaches:

The method according to claim 30, wherein the encrypted data information is stored in a memory, and wherein the stored data information is accessed by a processor.

[see rejection of claim 1]

As per claim 37, Rarick teaches:

The method according to claim 30, wherein the rolling comprises rotating bits within one or more rolling regions of the data information.

[see rejection of claim 3]

As per claim 38:

The system according to claim 1, wherein memory and the processor are part of a set top box, wherein the memory comprises a flash memory and an SDRAM, wherein

instructions are stored in the flash memory before being moved to the SDRAM for execution by the processor, and wherein the instructions stored in the flash memory are compressed before being moved to the SDRAM for execution by the processor.

[see Perego, col. 8, lines 39-67]

As per claim 39, Rarick teaches:

The system according to claim 1, wherein the processor uses a single pipeline stage decryption algorithm.

[see paragraph 57]

As per claim 40:

The system according to claim 1, wherein encrypted data stored in the memory has been encrypted using an encryption algorithm that varies periodically at address multiples such that repeated instructions are not encoded in the same way each time.

[see rejection of claim 1, wherein Watanabe teaches changing the key randomly or periodically]

As per claim 41, Rarick teaches:

The system according to claim 1, wherein the encrypted data stored in the memory is encrypted in a single clock cycle encryption scheme, and wherein the processor decrypts the encrypted data in a single clock cycle decryption scheme.

[see paragraph 71]

As per claim 42, 43:

The system according to claim 1, wherein the memory and the processor are part of a set top box, and wherein the processor that fixedly bit shuffles the bit-rolled data is configured as a fixed, hard-coded bit shuffler in which the fixed, hard-coded bit shuffling differs according to a class of the set top box such that different classes of set top boxes differ in their fixed, hard-coded bit shuffling.

[see Perego, col. 20, lines 35-50, wherein the keys are hard-wired. Examiner views this as resulting in the claimed "hard-coded bit shuffling]

As per claim 45, Rarick teaches:

The system according to claim 1, wherein the decryptor comprises a bit swapper and a bit roller, wherein the bit swapper is configured to provide fixed, hard-coded bit shuffling, wherein the bit roller is configured to provide variable bit rolling, wherein the decryptor comprises a plurality of two-bit adders, wherein each two-bit adder receives two bits from a bit swapper that received two bits from the bit roller, and wherein each two-bit adder receives two bits of the first key.

[see above rejections of claims 1 and 10]

As per claim 46, Rarick teaches:

The system according to claim 1, wherein a particular two-bit adder of the plurality of two-bit adders receives a different two bits of the first key based on different data addresses received by the processor.

[see paragraph 40]

As per claim 47, Rarick teaches:

The system according to claim 1, wherein each two-bit adder outputs two bits that are received in an XOR block, and wherein the XOR block receives two bits of the second key.

[see paragraph 40]

As per claim 48, Rarick teaches:

The system according to claim 47, wherein an output of the XOR block is decrypted data.

[see paragraph 40]

As per claim 49, Rarick teaches:

The system according to claim 48, wherein the decrypted data is stored in an internal memory of the processor.

[see fig. 11, register unit]

As per claim 50, Rarick teaches:

The system according to claim 1, wherein the second key is unrelated to the first key.

[see rejection of claim 1, wherein the second key changes randomly]

As per claim 54, Rarick teaches:

The system according to claim 50, wherein the decryptor comprises a bit swapper that swaps bits output from the variable bit roller, and wherein the decryptor comprises an adder that adds the shifted key to bits output from the bit swapper.

[see paragraph 40, "adders" and rejection of claim 1, "bit swap"]

As per claim 55, Rarick teaches:

The system according to claim 50, wherein the decryptor comprises an XOR block that processes bits output from the adder and bits from a hidden key that is unrelated to the shifted key, and wherein bits output from the XOR block are decrypted.

[see paragraph 40, "XOR" and "adders" and see rejection of claim 1, wherein the second key is viewed as the claimed hidden key]

As per claim 56, Rarick teaches:

The system according to claim 1, wherein the encrypted data is partitioned into a plurality of roll regions, the roll regions being of variable length, wherein each roll region is characterized by a roll skip, a roll region length and a roll amount, wherein the roll skip, the roll region length and the roll amount are set through bits of a portion of the original key, and wherein the bits of the portion of the original key, selected based on the data address, are used to set the roll skip, the roll region length and the roll amount.

Paragraph 32 of the Rarick reference teach the swap operation. Rarick teaches "the value present in the S[3] array position is written into the S[2] position, the value in the S[2] position is written into the S[1] position, the value in the S[1] position is written into the S[0] position, and so on." Examiner contends that this shifting of the values in the array is analogous to rolling as cited by applicant.

As per claim 57, Rarick teaches:

The system according to claim 1, wherein the bits of the portion of the original key used to set the roll skip, the roll region length and the roll amount are set using the bits of the portion of the original key which change as the data address changes.

[see paragraph 11]

POINTS OF CONTACT

*. Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulaney Street
Alexandria, VA 22314

*. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel L. Hoang whose telephone number is 571-270-1019. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Daniel L. Hoang/

Examiner, Art Unit 2436

/Eleni A Shiferaw/

Primary Examiner, Art Unit 2436